(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43344 A1

(51) International Patent Classification⁷: H04L 9/32

(21) International Application Number: PCT/US00/33606

(22) International Filing Date:
12 December 2000 (12.12.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/460,022 13 December 1999 (13.12.1999) US

(71) Applicant: RSA SECURITY INC. [US/US]; 36 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventor: KALISKI, Burton, S., Jr.; 22 Pembroke Road, Wellesley, MA 02482 (US).

(74) Agent: HEFFAN, Ira, V.; Testa, Hurwitz & Thibeault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

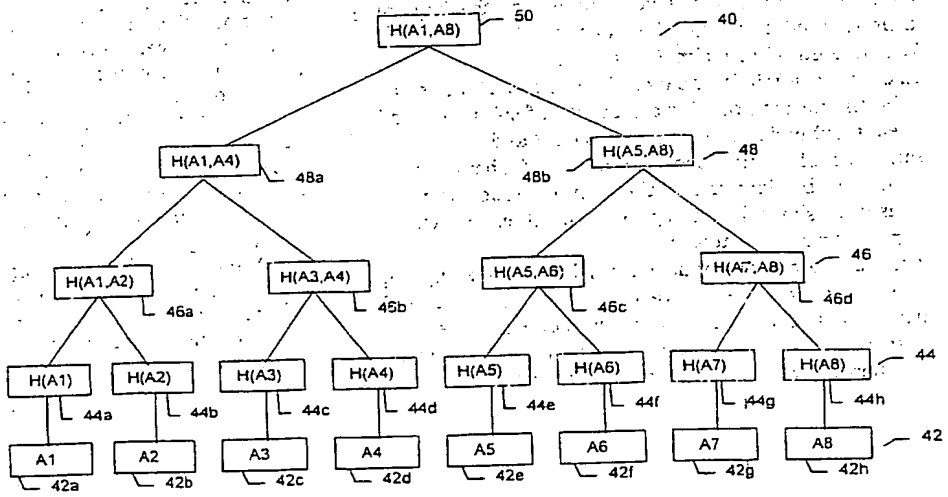
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR GENERATING AND MANAGING ATTRIBUTE CERTIFICATES



(57) Abstract: The system and method provide for an attribute certificate for a user based on a hash tree of attribute data. Typically, a user of a client system makes a request to an attribute authority system to provide a set of attribute data (42 a-h) used to provide the user with access to one or more resources, such as a computer system or database. The attribute authority generates a hash tree (40) with a hashed root (50) from the full set of attribute data for a user. The attribute authority generates an attribute certificate that includes a digital signature calculated from the root (50), and, optionally, the value of the root (50) itself. The attribute authority also provides verification data for the set of attribute data requested by the user. Typically, the attribute authority responds to a user's request by transmitting the attribute certificate (42 a-h), the verification data, and the requested set of attribute data to the client, which in turn sends the transmitted information to one or more resources to allow access by the user to the resources.

WO 01/43344 A1

System and Method for Generating and Managing Attribute Certificates

Field of the Invention

The invention relates generally to the field of computer security and authentication and, more particularly, to a system and method for generating and managing attribute certificates.

Background of the Invention

Certificates are used in the field of computer security. For example, certificates are used in the process of authenticating a user and allowing the user to access a computer or to access specific resources located on the computer or over a network.

An attribute certificate is a form of digital credential that binds identification information about a user and user attributes. The identification information may be a name, a public key, a reference to another certificate, other information, or a combination of the foregoing. A public key may be used as part of a public/private key cryptography system, such as a system based on RSA public/private key cryptography.

Attributes are additional information about a user and often specify authorization data, such as the authorization to use a particular computer system or other resource. A common form of authorization data is an encrypted password, where the password grants access to the resource, and is encrypted in a way that only the resource can obtain it. An attribute certificate is typically issued by a computer system or server referred to as an attribute authority, and the attribute certificate typically includes a digital signature of the attribute authority on the contents of the certificate.

Typically, a small number of attribute certificates, perhaps only one, is associated with a user, and such an attribute certificate is often valid for a relatively short period of time, such as 24 hours. The user typically requests an attribute certificate from an attribute authority after authenticating or otherwise interacting with the attribute authority via a network, such as an intranet or the Internet. This request typically happens when a user first needs access to a resource, for example, when a worker first begins her work day. In the request, the user specifies that the attribute certificate include authorization data for a selected set of resources. This selected set of resources may be smaller than the full set of resources that the user is allowed

access to. If the user later wishes to access a resource not in the selected set of resources, then the user must request another attribute certificate.

The user may not wish to request a full set of authorization information because the resulting attribute certificate may be very large. In addition, the user may not wish to disclose the full set of the user's allowed resources to other users or resources, for example, in the interest of privacy, security, or anonymity.

An attribute authority may pregenerate attribute certificates, when possible, to reduce the computational load at peak times, such as when many users are logging in at the beginning of the work day. However, it is difficult for the attribute authority to pregenerate attribute certificates if the attribute authority does not know the user's desired selection until the user requests it. For example, an attribute authority may pregenerate an attribute certificate for a user, based on what the user typically selects as a set of resources. However, if the user requests an attribute certificate for a different set of resources, the attribute authority must newly generate the attribute certificate. Alternatively, the attribute authority could pregenerate many different attribute certificates for a user based on many different sets of resources that could potentially be selected by the user. This approach may unnecessarily consume computational resources and data storage space for a large number of pregenerated attribute certificates.

Summary of the Invention

One object of the invention is to provide a system and method for generating attribute certificates that allows for the efficient pregeneration of attribute certificates, wherein only one attribute certificate need be generated per user, even though the user may request access to different subsets of resources at different times. Another object of the invention is to distribute only the attributes required to access a selected resource, without distributing unnecessarily other attribute data for the user. A further object is to limit the size of the attribute certificate as well as any verification data needed to verify the attribute data for a selected resource.

In one aspect, the invention relates to a method for providing attribute information to a user, the attribute information providing the user with access to a resource. The method includes generating a hash tree having a root from attribute data associated with a user; selecting a set of the attribute data; determining verification data capable of verifying the set of attribute data in the hash tree; calculating a digital signature using the root as input; generating an attribute certificate including the digital signature; and transferring the attribute certificate, the verification data, and the set of the attribute data to the user.

In one embodiment, the method includes generating an attribute certificate including the root and the digital signature. In another embodiment, the method includes allocating the attribute data to the leaves of the hash tree and determining verification data for one or more leaves of the hash tree. In a further embodiment, the attribute certificate is generated independently of a request by the user. In another embodiment, the attribute certificate includes the root of the hash tree, the verification data, and the digital signature. In another embodiment, the method includes encrypting the set of the attribute data, or a subset of the attribute data, before transferring the attribute certificate, the verification data, and the set of attribute data to the user.

In another aspect, the invention relates to an attribute authority for providing attribute information to a user, the attribute information providing the user with access to a resource. The attribute authority includes attribute data for a user, a hash tree generated based on the attribute data, an attribute certificate including a digital signature calculated using a root of the hash tree as input, and verification data capable of verifying a set of the attribute data in the hash tree. The attribute authority transfers the attribute certificate, the verification data, and the set of the attribute data to the user.

In one embodiment, the attribute certificate includes the root and the digital signature. In another embodiment, the hash tree includes leaves of attribute data, and the verification data includes verification data for one or more leaves of the hash tree. In a further embodiment, the attribute authority generates the attribute certificate independently of a request by the user. In another embodiment, the attribute certificate includes the root of the hash tree, the verification data, and the digital signature. In another embodiment, the attribute information includes the attribute certificate, the verification data, and an encrypted set of the attribute data.

In another aspect, the invention relates to a method for verifying attribute information received from a user. In one embodiment, the method includes receiving an attribute certificate including a digital signature calculated using as input an initial root of a hash tree that is generated from attribute data associated with a user; receiving a set of the attribute data; receiving verification data associated with the set of the attribute data; verifying the set of the attribute data using the attributed certificate and the verification data; and allowing access to a resource after verifying the set of the attribute data.

In another aspect, the invention relates to a system for verifying attribute information received from a user, including an input interface for receiving an attribute certificate, a set of

attribute data associated with a user, verification data used to verify the set of attribute data, and a verifier in electrical communication with the input interface. In one embodiment, the attribute certificate includes a digital signature calculated using as input an initial root of a hash tree that is generated based on attribute data. The input interface receives the attribute certificate, the set of the attribute data, and the verification data from the user, and the verifier allows access to a resource based on the verification of the set of the attribute data using the attribute certificate, and the verification data.

In another aspect, the invention relates to a method for using attribute information to obtain access to a resource. In one embodiment, the method includes receiving an attribute certificate including a digital signature calculated using as input a root of a hash tree generated based on attribute data for a user; receiving the attribute data; receiving verification data capable of verifying the attribute data; transferring to a resource the attribute certificate, the attribute data, and the verification data; verifying the attribute data using the attribute certificate and the verification data; and obtaining access to the resource in response to verifying the attribute data.

In one embodiment, the method includes receiving a set of attribute data and set of verification data capable of verifying the set of attribute data. In a further embodiment, the method includes transferring to the resource a subset of the attribute data and subset verification data capable of verifying the subset of the attribute data, and verifying the subset of the attribute data with the subset verification data.

In another aspect, the invention relates to a system for using attribute information to enable a user to obtain access to a resource. In one embodiment, the system includes a client associated with a user, an attribute authority, and a verifier capable of verifying the set of the attribute data using the attribute certificate and the verification data. In one embodiment, the attribute authority includes an attribute certificate including a digital signature calculated using as input a root of a hash tree generated based on attribute data for the user, a first set of the attribute data, a second set of the attribute data based on the first set of the attribute data, first verification data capable of verifying the first set of the attribute data, and second verification data capable of verifying the second set of the attribute data. The attribute authority transfers the attribute certificate, the first set of the attribute data, and the first verification data to the client. The client then transfers the attribute certificate, the second set of the attribute data, and the second verification data to the verifier, and the verifier provides the client with access to a resource

based on verification of the second set of the attribute data using the attribute certificate and the second verification data.

In one embodiment, the first set of attribute data and the second set of attribute data are the same set. In a further embodiment, the second set of attribute data is a subset of the first set of attribute data.

In a further aspect, the invention relates to an attribute certificate, including a root of a hash tree generated from attribute data for a user, and a digital signature calculated using the root as input. In one embodiment, the hash tree includes leaves, and the leaves include the attribute data.

In another aspect, the invention relates to attribute information for providing a user with access to a resource, including an attribute certificate including a digital signature calculated using as input the root of a hash tree generated from attribute data for the user and verification data capable of verifying a set of the attribute data. In one embodiment, the verification data includes authentication path data identifying a path from the root to one or more leaves of the hash tree. In another embodiment, the verification data includes hash tree node values.

Brief Descriptions of the Drawings

The invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description taken in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates a functional block diagram of an attribute certification system according to one embodiment of the invention.

FIG. 2 illustrates a functional block diagram of a verification system for verifying attribute information received from a user for one embodiment of the invention.

FIG. 3 illustrates a diagrammatic view of a hash tree of attribute information for one embodiment of the invention.

FIG. 4 illustrates a flow chart of the process of generating an attribute certificate, a set of attribute data, and verification data for one embodiment of the invention.

FIG. 5 illustrates a portion of the hash tree of FIG. 3, including verification data.

Detailed Description of the Invention

Figure 1 illustrates an embodiment of an attribute certification system 10 that provides attribute information from an attribute authority 12. The attribute information enables a client system 14 to obtain access to a resource 16. In one embodiment, the attribute information

includes an attribute certificate 22, a set of attribute data 24 used to access one or more resources 16, and verification data 26 used to verify the set of attribute data.

Typically, a user 15 is associated with the client system 14. In one embodiment, the user 15 is physically located at a client computer system 14 and uses the client 14 to access an attribute authority server computer 12 and a resource server computer 16 over a network. More specifically, the client 14, on behalf of the user 15, requests 20 an authorization credential from the attribute authority 12 that can be used to access the resource 16. The authorization credential is based on attribute data associated with the user 15. In one embodiment, the authorization credential is an attribute certificate 22. The resource 16 includes a verifier 18 for verifying the authorization credential provided by the client 14 to the resource 16.

In one embodiment, the client system 14 may be a personal computer, workstation or hardware security device in communication with the attribute authority 12 and the resource 16. In one embodiment, the user 15 is using another computer system, such as a remote computer system on a network that is in communication with the client 14. In another embodiment, the client 14 obtains the authorization credential on behalf of the user 15 at a specific time, such as early in the morning before the user 15 arrives at the client 14 to start the working day. The client 14 authenticates the user 15 before providing the authorization credential to the user 15 or using it on behalf of the user 15. An additional benefit is that the attribute authority 12 can pregenerate the authorization credentials in advance of a request by the user 15.

In one embodiment, the user 15 is not limited to a human user communicating with a computer system. In this embodiment, the user 15 is an entity that requests an authorization credential. For example, in one embodiment, the user 15 may be a software program, collection of software programs, software object, software agent, UNIX daemon, or other software construct, executing on the same or a different computer than the client 14. For example, the user 15 may be a mail daemon that requests authorization to send electronic mail to one or more recipients. In another embodiment, the user 15 is a hardware electronic circuit, integrated chip, ASIC (application specific integrated circuit), or robot. In a further embodiment, the user 15 is an AI (artificially intelligent) entity. In one embodiment, the user 15 is a digital computer. In another embodiment, the user 15 is an analog, nanotechnology-based, optical or other type of computer. In a further embodiment, the user 15 is a software agent acting on behalf of a human operator of a computer to search, purchase, or perform other functions over a network, such as

the Internet. In a further embodiment, the user software 15 is an integrated part of the client system 14.

The attribute authority 12, the client 14, and the resource 16 may be connected in a local computer network, direct cable or wire connection, modem connection, global network such as the Internet, or other connection allowing communication of data among the attribute authority 12, the client 14, and/or resource 16. Communications among the attribute authority 12, client 14, and resource may be based on electrical, microwave, infrared, optical, acoustic, or other communication mechanisms.

In one embodiment, the resource 16 is a computer system, a database, or other resource that the user 15 desires to connect to through the client 14. In one embodiment, the resource 16 provides computational resources or data that the user 15 needs. In another embodiment, the resource 16 is a physical location or entity that the user 15 desires to access or use, such as a room, a locked automobile, or the locked ignition mechanism for an automobile.

In another embodiment, the verifier 18 verifies attributes of the user 15. In another embodiment, the verifier 18 verifies the authorization of the user 15 to take certain actions, such as authority to commit a company to engage in transactions by the user 15 acting as an agent of the company.

In one embodiment, the verifier 18 is part of the resource 16. In another embodiment, the verifier 18 is electronically connected to the resource 16, but is not part of the resource 16. In one embodiment, the verifier 18 is a software program executing on an independent computer system. In another embodiment, the verifier 18 is a software program executing on a resource computer system 16. In a further embodiment, the verifier 18 is a hardware integrated circuit or device, such as an ASIC.

The attribute authority 12 stores or has access to attribute data that is associated with the user 15. The attribute data includes information that can be used to access a large number of different resources 16. For example, a user 15 could potentially use the client 14 to access 1000 or more resources 16. The attribute authority 12 would have attribute data associated with each resource 16.

In one embodiment of the invention, the user 15 uses the client 14 to make a request 20 for authorization information, such as attribute information and/or an attribute certificate, for access to only one resource 16. In another embodiment, the user 15 may use the client 14 to

request access to two or more resources 16. In another embodiment, the client 14 makes the request 20 without the user 15 making an explicit request. Rather, the client automatically requests access based on another action taken by a user 15, for example, commencement of a particular software application. The attribute authority 12 responds to the request 20 and provides input information to the client 14, including an input attribute certificate 22, an input set of attribute data 24 that is used to access the resource 16, and input verification data 26, which can be used to verify the input set of attribute data 24.

After receiving the input information the client 14 then transfers output information to the verifier 18 of the resource 16, including an output attribute certificate 28, an output set of attribute data 30, and output verification data 32. In one embodiment, the user 15 requests the client 14 to send the output information. In another embodiment, the client 14 automatically sends the output information upon receiving the input information. In another embodiment, the client 14 receives the input information at one point in time, stores it, and provides the output information to the verifier 18 at another point in time. After receiving the output information, the verifier 18 verifies the output set of attribute data 30 using the output attribute certificate 28 and the output verification data 32 provided by the client 14. If the verification is successful, the verifier 18 then allows the client 14 to access 34 the resource 16.

In one embodiment, the input set of attribute data 24 includes attribute data for one or more resources 16, up to the complete set of attribute data that the user 15 can possibly access. That is, if the user 15 can access up to 1000 resources 16, the input set of attribute data 24 can include attribute data for between 1 and 1000 resources 16. In one embodiment, the output set of attribute data 30 is the same set of attribute data as the input set 24. In another embodiment, the output set of attribute data 30 is a subset of the input set of attribute data 24.

In another embodiment, the input attribute certificate 22 includes the input verification data 26 or a portion of the verification data 26. In a further embodiment the output attribute certificate 28 includes the output verification data 32 or a portion of the output verification data 32.

FIG. 2 illustrates a functional block diagram of a verification system for verifying attribute information received from a user 15, including a user 15, a resource 16, and a verification system 36 for one embodiment of the invention. The verification system 36 includes a verifier 18 and an input interface 34 for receiving the output attribute certificate 28, output set

of attribute data 30, and output verification data 32 from the user 15. The verifier 18 verifies the output set of attribute data 30 and allows the user 15 access 34 to the resource 16.

In one embodiment, the user 15 has previously obtained the output information, that is, the attribute certificate 28, the attribute data 30, and verification data 32, and then stored the output information in a storage medium, such as a hard disk, diskette, or CD-ROM or memory element, such as ROM or RAM. The user 15 then recovers the output information from the storage medium and provides it to the input interface 34. In another embodiment, the user 15 has the output information stored on a smart card or other device that can be read by the input interface 34. In one embodiment the smart card is a PC card, such as a PCMCIA (Personal Computer Memory Card International Association) card.

In one embodiment, the user 15 is seated at a computer system and uses the computer system to transfer the output information to the verification system 36. In one embodiment, the user 15 is using a computer or other device, and the user's computer, the resource 16, and the verification system 36 are connected electronically, such as in a computer network, by modem, or other electrical communication. In another embodiment, the computer system used by the user 15 is a client computer system 14 used in a manner similar to that shown in FIG. 1 and discussed previously.

In one embodiment, the input interface 34 is a network interface connected through a network to a computer system or other device operated by the user 15. In another embodiment the input interface 34 is any suitable communication interface, such as a keyboard, mouse, serial port, modem interface or other interface for communicating with computers or other hardware devices. In a further embodiment, the input interface 34 is a security device capable of reading a portable storage medium provided by the user 15, such as a diskette, CD-ROM, smart card, or smart token. In another embodiment, the input interface 34 is a device capable of receiving optical, video, or other transmissions.

In one embodiment, the input interface 34 and the verifier 18 are part of the verification system 36. In one example, the verification system 36 is a computer system. In one embodiment, the verification system 36 and the resource 16 are part of the same system, such as one computer system. In another embodiment, the verification system 36 and resource 16 are separate systems connected by a communications link such as an electronic link (not shown in FIG. 2).

FIG. 3 illustrates a diagrammatic view of a hash tree 40 of leaves of attribute data 42 in one embodiment of the invention. The hash tree 40 can be constructed by a generally known process, such as described in U.S. Patent No. 4,309,569 "Method of Providing Digital Signatures" to Merkle, which provides a detailed discussion of hash trees.

In FIG. 3, the outermost leaves of the hash tree 40 are represented by leaves A1 through A8 of attribute data 42a, 42b, 42c, 42d, 42e, 42f, 42g, 42h (referred to generally as 42). Each leaf of attribute data 42 includes a quantity of attribute data 42. In one embodiment, each leaf of the attribute data 42 is associated with one resource 16 that the user 15 has authorization to access, and may include such information related to that resource 16 as a password that provides access to that resource 16. In another embodiment, each leaf of attribute data 42 is not required to be associated with one resource 16, but several leaves of attribute data 42 may represent one resource 16. In another embodiment, each leaf of attribute data 42 includes attribute data 42 for several resources 16. In a further embodiment, the attribute data 42 may include privilege or group membership information applicable to multiple resources. The resources recognize that membership in a certain group carries with it an authorization associated with that group.

A first level of hash tree nodes 44 is formed by calculating a one-way "hash" function on each leaf of attribute data 42 to produce first level nodes 44 illustrated by 44a through 44h with associated hash values H(A1) through H(A8) in FIG. 3. Each first level node 44 is the resultant hashed value of applying the one-way function to the attribute data. Thus, the value of node 44a is the hashed value H(A1) determined by applying the one-way function to the attribute data in leaf 42a. The one-way hash function can be any one of commonly used and known one-way functions known in the field of cryptography. In addition to the function being a one-way function, a collision resistant property may also be desirable. In one embodiment, the one-way function is the SHA (Secure Hash Algorithm) described in the SHS (Secure Hash Standard) of the NIST (National Institute of Standards and Technology) NIST FIPS PUB 180-1, "Secure Hash Standard" U.S. Department of Commerce, April 17, 1995. Another one-way function that may be used in another embodiment of the invention is MD5 as described in R.L. Rivest, "The MD5 Message Digest Algorithm," IETF (Internet Engineering Task Force) RPC (Request for Comments) 1321, April 1992. An additional one-way hash function that may be used in another embodiment of the invention is RIPEMD-160, as described in H. Dobbertin, A. Bosselaers and B. Preneel, "RIPEMD-160: A Strengthened Version of RIPEMD," in D. Gollmann, Editor, Fast

Software Encryption, pp.71-82, Lecture Notes in Computer Science 1039, Springer-Verlag, 1996 (or see http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html).

A second level of hash nodes 46 is formed by calculating the one-way hash function on the values of the first level nodes 44. Thus, in FIG. 3, for node 46a, the value H(A1,A2) represents the hashed value of applying the hash function to the values H(A1) and H(A2) in the nodes 44a and 44b in the first level of nodes 44. In one embodiment, the values H(A1) and H(A2) can be concatenated together and the one-way function then applied to the concatenated value. In other embodiments, other methods of hashing may be used to produce a resultant hashed value, H(A1,A2), from two input values, such as the hashed values H(A1) and H(A2). In another embodiment, the approach used is the one described in U.S. Patent No. 4,309,569 to Merkle to produce the hashed value of H(A1,A2) from the values of H(A1) and H(A2). In a further embodiment, the resultant hashed value may be based on multiple values, such as multiple hashed values or multiple leaves of attribute data 42.

A third level of hash nodes 48 is formed by calculating the one-way hash function on the values of the second level nodes 46. In FIG. 3, the notation H(A1,A4) for node 48a is used to represent the resultant hash value that results from applying a hash function to the values H(A1,A2) and H(A3,A4) in the nodes 46a and 46b. Thus, H(A1,A4) is a single hashed value that represents the attribute data A1 through A4 contained in leaves 42a through 42d.

FIG. 3 shows one example only. The number of leaves, nodes, and branches shown in the example is illustrative, and is not intended to limit the invention to a specific implementation. For example, a hash tree 40 can have more or less than eight leaves of attribute data 42. For a larger hash tree 40, additional levels of hashed node values beyond the levels 44, 46, 48 shown in FIG. 3 can be calculated, such as fourth, fifth, and additional levels, as required by the size of the hash tree 40. In one embodiment, the hash tree is not required to be balanced, but some branches may have more nodes than other branches. The general structure of the tree is that of a directed graph with a root.

At the base of the hash tree 40, a single hashed value is calculated to represent all of the leaves of attribute data 42. In FIG. 3, this fourth node level, or root, 50 is illustrated by node H(A1,A8), which is calculated from the values of the third level nodes 48a and 48b, that is, H(A1,A4) and H(A5,A8).

Because the hash tree is a set of one-way values, when the authority 12 signs the root 50, it is as if it signed the whole tree. The short path from any leaf to the root 50, even if there are many leaves of attribute data 42, minimizes the calculations necessary to verify a leaf.

As described above for FIG. 1, a user 15 or client 14 receives an attribute certificate 22, attribute data 24, and verification data 26 from the attribute authority 12. In one embodiment, attribute data 42 are allocated to the leaves of the hash tree 40 as described above for FIG. 3, and the hash tree 40, including the root 50, is calculated from the attribute data 42. The attribute certificate 22 includes a digital signature calculated using the root 50 as input. In one embodiment, the client 14 receives the selected leaves of the attribute data 42 as the input set of attribute data 24. Verification data 28 includes a portion of the hash tree 40 that is sufficient, along with the selected leaves of attribute data 42, to verify the root 50, as described in more detail below. In one embodiment, the client 14 provides output information to the verifier 18 including the output attribute certificate 28, the output set of attribute data 30, and the output verification data 32. The verifier 18 uses the attribute certificate 28 and the verification data 32 to verify the set of attribute data 30 to allow access to a resource 16.

In another embodiment, as shown in FIG. 2, the user 15 receives the selected leaves of the attribute data 42 and provides the attribute certificate 28, the set of attribute data 30, and the verification data 32 to the verification system 36.

FIG. 4 illustrates a flowchart of the process of generating the input attribute certificate 22, the input set of attribute data 24, and the input verification data 26. First, the attribute authority 12 creates a hash tree 40 based on all of the attribute data 42 associated with a user 15, including the calculation of the root 50 of the hash tree 40 (step 100). In another embodiment, the hash tree 40 is based on a subset of the attribute data 42, with different hash trees 40 for each subset of the attribute data 42. The attribute authority 12 calculates a digital signature using the root 50 of the hash tree 40 as input (step 102) possibly as well as other elements such as the user's name, the attribute authority's name, and a date. In one embodiment, the digital signature is calculated using the private key of the attribute authority 12 in a public/private key system. In another embodiment, the attribute authority 12 uses any other digital signature method that provides for a digital signature calculation using the root 50 as input. In one embodiment, the attribute authority 12 uses a digital signature scheme based on PSS (probabilistic signature scheme). In this approach, a signature is appended to the data that is signed (the root 50 and possibly other elements), and the verification operation is applied to the signature and the data that is signed. In another embodiment, a PSS-R (PSS-recovery) approach is used, and some or all of the data that is signed (the root 50 and possibly other elements) can be recovered from the digital signature. The attribute authority 12 then creates an attribute certificate 22 that includes the digital signature

(step 104) and possibly other elements. In one embodiment, the attribute certificate 22 includes the digital signature, but does not directly include the root 50, although the root 50 is included indirectly because the digital signature is calculated using the root 50. In another embodiment, the attribute certificate 22 includes the root 50 directly along with the digital signature.

The attribute authority 12 selects a set of input attribute data 24 based on the user's 15 request for those resources 16 the user 15 wishes to access (step 106). The attribute authority 12 determines the verification data that the client 14 can send to the verifier 18 as output verification data 32. The verifier 18 verifies the output set of attribute data 30 using the output attribute certificate 28 and output verification data 32 received by the verifier 18 from the client 14 (step 108). In one embodiment, the input attribute certificate 22, the input set of attribute data 24, and the input verification data 26 are the same as the output attribute certificate 28, the output set of attribute data 30, and the output verification data 32. In another embodiment, any or all on the input information to the client 22, 24, 26 is derived from or otherwise different from the output information 28, 30, 32.

In one embodiment, the attribute authority 12 uses the hash tree 40 to determine the input verification data 26. The client 14 must provide sufficient information in the output verification data 32 so that the verifier 18 can determine a calculated root of the hash tree 40 which is then compared to the initial root 50 of the hash tree 40. If the attribute certificate 22 includes the root 50 along with the digital signature, or the root 50 can be recovered from the digital signature in the case of a signature scheme with message recovery, then the verifier 18 verifies the digital signature on the attribute certificate 22, recovers the root 50 from the digital signature if necessary, and compares the calculated root of the hash tree 40 with the initial or recovered root 50 associated with the attribute certificate 22. If the digital signature is valid and the calculated root and the initial or recovered root 50 are substantially similar or equal, then the verifier 18 can authenticate the user 15 and allow for access by the user 15 to the resource 16. In this approach, the verifier 18 may verify the digital signature on the attribute certificate 22 separately from processing the hash tree 40, which is convenient because it is similar to how attribute certificates 22 without hash trees 40 are verified in existing systems.

In another embodiment, if the attribute certificate 22 does not include the root 50 and the root 50 cannot be recovered from the digital signature, then the verifier 18 verifies the digital signature on the attribute certificate 22 with the calculated root as input. If the digital signature is valid, then the verifier is assured that the calculated root and the initial root 50 are substantially

similar or equal, and the verifier 18 can authenticate the user 15 and perform further processing as above.

The verifier 18 may also wish to authenticate the user 15 for any of a variety of conventional authentication mechanisms, such as a password provided by a user 15, or a challenge and response approach.

For example, referring again to FIG. 3, suppose the user 15 requests, through the client 14, the attribute data A8 associated with leaf 42h. The verifier 18 receives this data from the client 14 as the output set of attribute data 30 (FIG. 1), but the verifier 18 can only calculate the first level hash node 44h from the data A8 in leaf 42h (see FIG. 3). The output verification data 32 must include enough information about other nodes in the hash tree 40 to allow the verifier 18 to calculate a calculated root equal to the initial root 50. This is shown in FIG. 5.

FIG. 5 illustrates a portion of the hash tree 40 of FIG. 3, including the leaves and nodes of the hash tree that could be used as verification data 32 for attribute data A8. The verification data 32, as shown in FIG. 5, includes the nodes 48a, 46c, and 44g. Using the hashed values from nodes 44g and 42h, the verifier 18 can calculate the hashed value in node 46d. Using the hashed value from node 46c from the verification data 32 and the hashed value from node 46d, the verifier 18 can calculate the hashed value for 48b. Using the hashed values from node 48a from the verification data 32 and node 48b, the verifier 18 can then determine a calculated root, which can be compared to the initial or recovered root 50 of the hash tree 40.

Node values such as 48a, 46c and 44g are referred to as an authentication path, which is a path of nodes in the hash tree 40 for a node of interest (such as 42h) sufficient to verify the attribute data in the node (such as attribute data A8 in node 42h) by providing enough nodes in the hash tree 40 to produce a calculated root, which can then be compared to the initial or recovered root 50. The root 50 is implicit in the construction of the hash tree 40, and the authentication path allows the root 50 to be reconstructed. If the node of interest (42h) can be thought of as a child node, then the authentication path can be thought of as a list of siblings, uncles and aunts, great-uncles and great aunts, and cousins such that the common ancestor or root 50 in the tree 40 can be identified.

In another embodiment, the attribute certificate 22 includes a root 50 and a partial verification data, such as a partial authentication path. This allows the verifier 18 to access the partial verification data directly from the attribute certificate 22 and thus simplifies validation of a portion of the hash tree 40. In this embodiment, additional verification data may be included in the separately transmitted verification data 32.

The authentication path can also be thought of as providing sufficient information to authenticate a path from the root to the leaf data of interest (such as 42h); that is, the verifier 18 can determine that 42h is a valid piece of attribute data in the hash tree 40, and therefore there must be a valid path from the attribute data 42h to the root 50.

The verification data 32, in the example given for FIG. 5, can include other nodes, such as 46a, 46b, 46c, and 44g (see FIG. 3), so long as enough nodes are provided to allow the verifier 18 to determine a calculated root of the hash tree 40 that can be compared to the initial or recovered root 50 received in the output attribute certificate 28. In one embodiment, the verifier 18 verifies more than one leaf of the tree 40. This may occur, for example, if several leaves of attribute data 42 are needed to access a resource 16.

An advantage of the embodiment described here is that the verifier 18 only receives the attribute data 42, such as A8, that is needed to access the resource 16. The verifier 18 does not receive the other attribute data 42 such as A1 through A7, which may be held secret and not distributed when not needed.

Also, the input attribute certificate 22 and output attribute certificate 28 are prevented from growing to an unmanageable size. For example, the attribute certificate 28 is not required to include all of the attribute data 42, but only a digital signature (or, in another embodiment, the root 50 and digital signature). The input verification data 26 and output verification data 32 are also restricted in size because they only need to include a sufficient number of hash values to determine a calculated root, and not every hash value or attribute value in the hash tree 40.

In addition, the hashed values for the hash tree 40 can be calculated independently of when the user 15 requests access 20 to a resource 16. Thus the input attribute certificate 22 can be precalculated. For example, when the user 15 requests access 20 to a resource 16 that requires attribute data A8, the attribute authority 12 is not required to calculate the associated hash values in the authentication path for A8. The attribute authority 12 does not have to recalculate a signature on the specified attribute data 42. For example, as shown in FIG. 5, hashed values of nodes, such as 48a, 46c, and 44g, can be precalculated, stored, and provided for the input verification data 26 for attribute data A8 in node 42h when needed.

In one embodiment of the invention, the attribute certificate 22 includes the user's public key. In alternate embodiments, the public key may be an attribute of the attribute certificate 22, or may be conveyed as a separate part of the attribute certificate 22. The client 14 then authenticates the user 15 to the verifier 18 by performing a cryptographic operation with the user's 15 corresponding private key, according to conventional protocols based on public-key

cryptography, as is known in the art. Using this approach, the set of verifiers 18 to which the client 14 may authenticate the user 15 is unlimited. However, it may be more efficient if the authentication is directed to a particular verifier 18, as described further.

In another embodiment, an attribute includes the encryption of a symmetric key with the verifier's 18 public key or with a key-encryption key shared by the attribute authority 12 and the verifier 18 using encryption techniques well known in the art. The attribute authority 12 provides the symmetric key to the client 14 in addition to the attribute information. The verifier 18 decrypts the attribute with its private key or the shared key-encryption key to recover the symmetric key. The client 14 then authenticates the user 15 to the verifier 18 by providing or by performing cryptographic operations with the symmetric key. The symmetric key should be changed periodically to prevent replay attacks, for instance each time a new attribute certificate 22 is issued.

In another embodiment of the invention, the system 10 is used with a secure channel, such as an SSL channel such as provided by the KeON system from RSA Security Inc. The secure channel provides for the secure transmission of data over the channel between computer systems. In one embodiment, this may be accomplished by a cryptographic approach. In another embodiment, the secure channel is a physical connection, such as a cable secured from physical tapping or monitoring of the transmission. The client 14 is connected to the attribute authority 12 and the resource 16 by the secure channel. In this embodiment, the set of attribute data 24, 30 can be transmitted without an additional stage of encryption and any sensitive data, such as passwords in the set of attribute data 24, 30 is protected from discovery during transmission by the secure channel. The verifier 18 that receives the attribute data 30 does not need to engage in a separate decryption step to obtain the password, as is the case when individual attributes are encrypted separately with the verifier's 18 public key. If the attribute authority 12 provides the sensitive data such as encrypted password to the client 14 in addition to the attribute information, the client 14 can then authenticate the user 15 to the verifier 18 by providing or performing cryptographic operations with the sensitive data. However, the sensitive data may also be used without the client's 14 participation. For instance, the sensitive data may include a password that the verifier 18 provides to the resource 16.

In another embodiment, the root 50 or value derived from it is provided by the attribute authority 12 to the client 14 through a secure channel, and then provided by the client 14 to

selected verifiers 18 through a secure channel, but is not generally made public. The root 50 or value derived from it thus provides a secure way of identifying and authenticating the user 15, assuming that the selected verifiers 18 can be trusted not to disclose the value. This approach is an improvement over the general approach where the root 50 or value derived from it is made public or is available to potentially untrusted verifiers 18, since in that case the attribute certificate 22 only authorizes but does not authenticate the user 15.

Having described the preferred embodiments of the invention, it will now become apparent to one of skill in the art that other embodiments incorporating the concepts may be used. It is felt, therefore, that these embodiments should not be limited to disclosed embodiments but rather should be limited only by the spirit and scope of the following claims.

CLAIMS

What is claimed is:

1. A method for providing attribute information to a user, the attribute information providing the user with access to a resource, comprising the steps of:

generating a hash tree from attribute data associated with a user, the hash tree comprising a root;

selecting a set of the attribute data;

determining, in response to the generated hash tree and the selected set of the attribute data, verification data capable of being used to verify the set of attribute data;

calculating a digital signature using the root as input;

generating an attribute certificate comprising the digital signature; and

providing the attribute certificate, the verification data, and the set of the attribute data to the user.

2. The method of claim 1, wherein the step of generating an attribute certificate comprises generating an attribute certificate comprising the root and the digital signature.

3. The method of claim 1, wherein the step of generating a hash tree comprises allocating the attribute data to leaves of the hash tree; and the step of determining the verification data comprises determining the verification data for at least one leaf of the hash tree.

4. The method of claim 3, wherein the step of determining the verification data comprises providing authentication path data enabling identification of a path from the root to the at least one leaf of the hash tree.

5. The method of claim 3 wherein the step of determining the verification data comprises providing hash tree node values.

6. The method of claim 3, wherein the step of generating the hash tree comprises generating a plurality of hash trees, and the step of generating the attribute certificate comprises generating the attribute certificate from at least one root of the plurality of hash trees.

7. The method of claim 1, wherein the step of generating the attribute certificate comprises generating the attribute certificate independently of a request by the user.

8. The method of claim 1, wherein the step of generating the attribute certificate comprises generating the attribute certificate comprising the root of the hash tree, the verification data, and the digital signature.

9. The method of claim 1, further comprising the step of encrypting the set of the attribute data before the step of transferring the attribute certificate, the verification data, and the set of the attribute data to the user, wherein the transferring step comprises transferring the encrypted set of the attribute data to the user.

10. An attribute authority for providing attribute information to a user, the attribute information providing the user with access to a resource, comprising:

attribute data for a user;

a hash tree generated based on the attribute data;

an attribute certificate comprising a digital signature calculated using a root of the hash tree as input; and

verification data determined in response to the generated hash tree and the attribute data for the user, the verification data capable of being used to verify a set of the attribute data in the hash tree,

wherein the attribute authority provides the attribute certificate, the verification data, and the set of the attribute data to the user.

11. The attribute authority of 10, wherein the attribute certificate comprises the root and the digital signature.

12. The attribute authority of claim 10, wherein the hash tree comprises leaves comprising the attribute data, and the verification data comprises the verification data for at least one leaf of the hash tree.

13. The attribute authority of claim 12, wherein the verification data comprises authentication path data enabling identification of a path from the root to the at least one leaf of the hash tree.

14. The attribute authority of claim 12, wherein the verification data comprises hash tree node values.

15. The attribute authority of claim 12, wherein the attribute certificate comprises at least one root of a plurality of hash trees generated based on the attribute data.

16. The attribute authority of claim 10, wherein the attribute authority generates the attribute certificate independently of a request by the user.

17. The attribute authority of claim 10, wherein the attribute certificate comprises the root of the hash tree, the verification data, and the digital signature.

18. The attribute authority of claim 10, wherein the attribute information comprises the attribute certificate, the verification data, and an encrypted set of the attribute data.

19. A method for verifying attribute information received from a user, comprising the steps of:

receiving an attribute certificate comprising a digital signature calculated using as input an initial root of a hash tree, wherein the hash tree is generated from attribute data associated with a user;

receiving a set of the attribute data;

receiving verification data associated with the set of the attribute data; verifying the set of the attribute data using the attribute certificate and the verification data; and

allowing access to a resource in response the step of verifying the set of the attribute data.

20. The method of claim 19, wherein the step of verifying the set of attribute data comprises determining a calculated root based on the verification data and the set of the attribute data, and verifying the digital signature using the calculated root as input.

21. The method of claim 19, wherein the step of verifying the set of attribute data comprises verifying the digital signature, determining the initial root from the attribute certificate, determining a calculated root based on the verification data and the set of the attribute data, and comparing the initial root and the calculated root.

22. The method of claim 19, wherein the step of verifying the set of attribute data comprises verifying the digital signature, determining a recovered root from the digital signature, determining a calculated root based on the verification data and the set of the attribute data, and comparing the recovered root and the calculated root.

23. The method of claim 19, wherein the step of receiving the attribute certificate comprises receiving the initial root and the digital signature.

24. The method of claim 19, wherein the step of allowing access comprises determining a recovered root from the digital signature and authorizing access to the resource by the user by using the recovered root and the verification data to authenticate the set of the attribute data.

25. The method of claim 19, wherein the step of allowing access comprises determining a calculated root based on the verification data and on the set of the attribute data, and comparing the calculated root and the initial root.

26. The method of claim 19, wherein the step of allowing access comprises determining authentication path data from the verification data and determining a direct path from the initial root to at least one leaf of the hash tree based on the authentication path data.

27. The method of claim 19, wherein the step of allowing access comprises determining hash tree node values from the verification data.

28. The method of claim 19, wherein the step of receiving the attribute certificate comprises receiving a plurality of initial roots of a plurality of hash trees and receiving a digital signature based on the plurality of initial roots.

29. The method of claim 19, wherein the step of receiving the attribute certificate comprises receiving the attribute certificate comprising the initial root of the hash tree, the digital signature, and the verification data.

30. The method of claim 19, wherein the step of receiving the set of the attribute data comprises receiving an encrypted set of the attribute data and decrypting the encrypted set of the attribute data.

31. A system for verifying attribute information received from a user, comprising:

an input interface for receiving from a user:

an attribute certificate comprising a digital signature calculated using as input an initial root of a hash tree generated based on attribute data;

a set of the attribute data associated with the user;

verification data for the set of the attribute data; and

a verifier in electrical communication with the input interface, the verifier capable of verifying the set of the attribute data using the attribute certificate and the verification data;

wherein the input interface transfers the attribute certificate, the set of the attribute data, and the verification data to the verifier, and the verifier allows access to a resource based on verification of the set of the attribute data using the attribute certificate, and the verification data.

32. The system of claim 31, wherein the verifier determines a calculated root based on the verification data and the set of attribute data, and verifies the digital signature using the calculated root as input.

33. The system of claim 31, wherein the verifier verifies the digital signature, determines the initial root from the attribute certificate, determines a calculated root based on the verification data and the set of the attribute data, and compares the initial root and the calculated root.

34. The system of claim 31, wherein the verifier verifies the digital signature, determines a recovered root from the digital signature, determines a calculated root based on the verification data and the set of the attribute data, and compares the recovered root and the calculated root.

35. The system of claim 31, wherein the attribute certificate comprises the initial root and the digital signature.

36. The system of claim 31, wherein the verifier authorizes access to the resource by the user by determining a recovered root from the digital signature and by using the verification data and the recovered root to authenticate the set of the attribute data.

37. The system of claim 31, wherein the verifier determines a calculated root using the verification data and the set of the attribute data as input, and compares the calculated root and the initial root.

38. The system of claim 31, wherein the verifier determines authentication path data from the verification data and determines a direct path from the initial root to at least one leaf of the hash tree using the authentication path data.

39. The system of claim 31, wherein the verifier determines hash tree node values from the verification data.

40. The system of claim 31, wherein the initial root is a plurality of initial roots of a plurality of hash trees and the verifier calculates the digital signature using the plurality of initial roots as input.

41. The system of claim 31, wherein the attribute certificate comprises the initial root of the hash tree, the digital signature, and the verification data based on the set of the attribute data.

42. The system of claim 31, wherein the set of the attribute data is an encrypted set of the attribute data and the verifier decrypts the encrypted set of the attribute data.

43. A method for using attribute information to obtain access to a resource, comprising the steps of:

receiving an attribute certificate comprising a digital signature calculated using as input a root of a hash tree, the hash tree generated based on attribute data for a user;

receiving the attribute data;

receiving verification data capable of verifying the attribute data;

transferring to a resource the attribute certificate, the attribute data, and the verification

data;

verifying the attribute data using the attribute certificate and the verification data; and

obtaining access to the resource in response to the step of verifying the attribute data.

44. The method of claim 43, wherein the step of receiving the attribute data comprises receiving a set of the attribute data; the step of receiving the verification data comprises receiving verification data capable of verifying the set of the attribute data; the step of transferring to the resource the attribute certificate, the attribute data, and the verification data comprises transferring to the resource the set of the attribute data; and the step of verifying the attribute data comprises verifying the set of the attribute data.

45. The method of claim 43, wherein the step of receiving the attribute data comprises receiving a set of the attribute data; the step of receiving the verification data comprises receiving set verification data capable of verifying the set of the attribute data; the step of transferring to the resource the attribute certificate, the attribute data, and the verification data comprises transferring to the resource a subset of the attribute data and subset verification data capable of verifying the subset of the attribute data ; and the step of verifying the attribute data comprises verifying the subset of the attribute data using the attribute certificate and the subset verification data.

46. The method of claim 43, wherein the step of receiving the attribute certificate comprises receiving the attribute certificate comprising the root and the digital signature.

47. A system for using attribute information to enable a user to obtain access to a resource, comprising:

a client associated with a user;

an attribute authority comprising:

an attribute certificate comprising a digital signature calculated using as input a root of a hash tree generated based on attribute data for the user;

a first set of the attribute data;

a second set of the attribute data based on the first set of the attribute data;

first verification data capable of verifying the first set of the attribute data, wherein the attribute authority transfers the attribute certificate, the first set of the attribute data, and the first verification data to the client; and

second verification data capable of verifying the second set of the attribute data,

a verifier capable of verifying the second set of the attribute data using the attribute certificate and the second verification data,

wherein the client transfers the attribute certificate, the second set of the attribute data, and the second verification data to the verifier, and the verifier provides the client with access to a resource based on verification of the second set of the attribute data using the attribute certificate and the second verification data.

48. A system as in claim 47, wherein the first set of the attribute data and the second set of the attribute data are the same set.

49. A system as in claim 47, wherein the second set of attribute data is a subset of the first set of attribute data.

50. A system as in claim 47, wherein the attribute certificate comprises the root and the digital signature.

51. An attribute certificate, comprising:

a root of a hash tree generated from attribute data for a user; and

a digital signature calculated using the root as input.

52. The attribute certificate of claim 51, wherein the hash tree comprises leaves and the leaves comprise the attribute data.

53. Attribute information for providing a user with access to a resource, the attribute information comprising:

an attribute certificate comprising a digital signature calculated using as input the root of a hash tree generated from attribute data for the user; and

verification data capable of verifying a set of the attribute data.

54. The attribute information of claim 53, wherein the verification data comprises authentication path data identifying a path from the root to at least one leaf of the hash tree.

55. The attribute information of claim 53, wherein the verification data comprises hash tree node values.

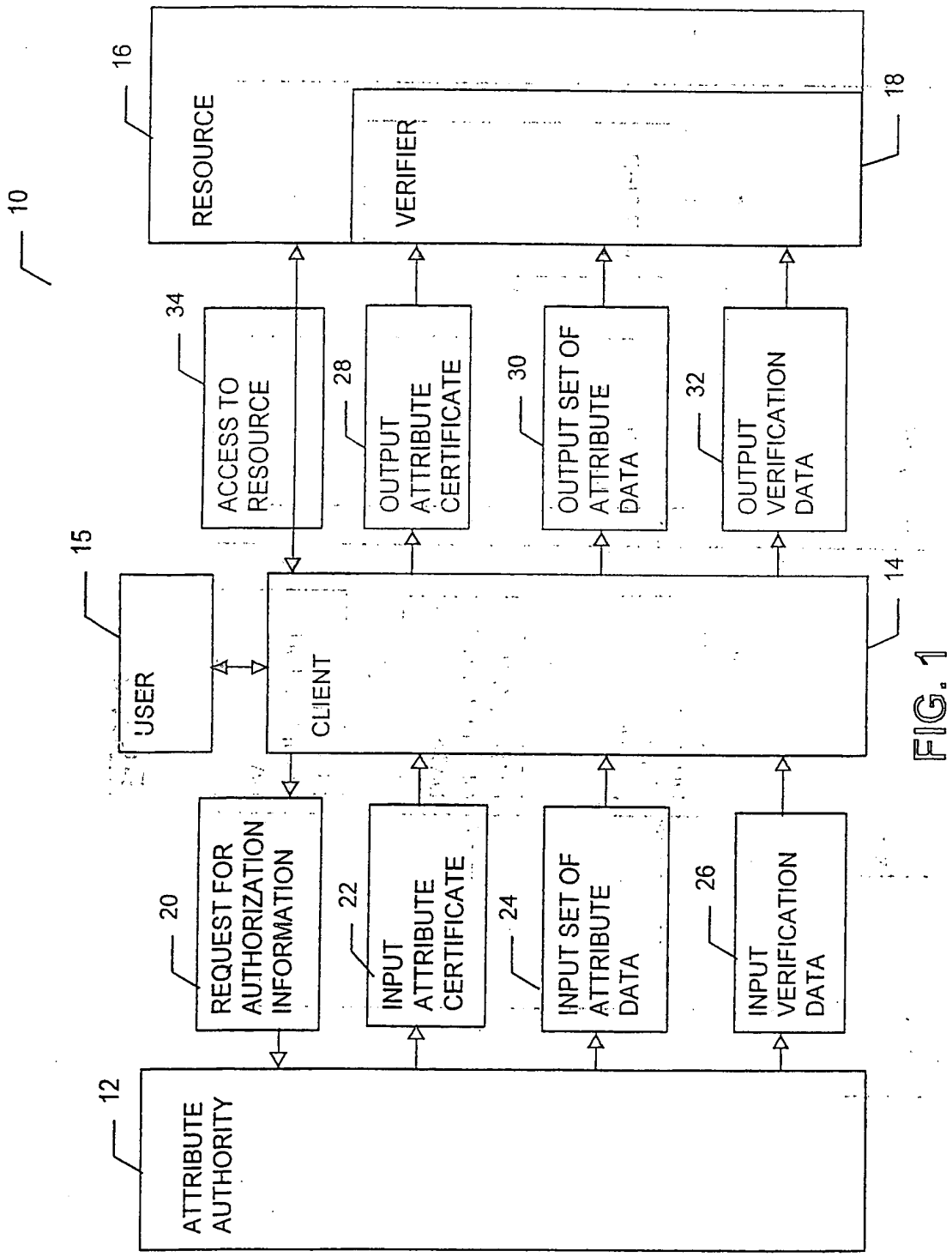


FIG. 1

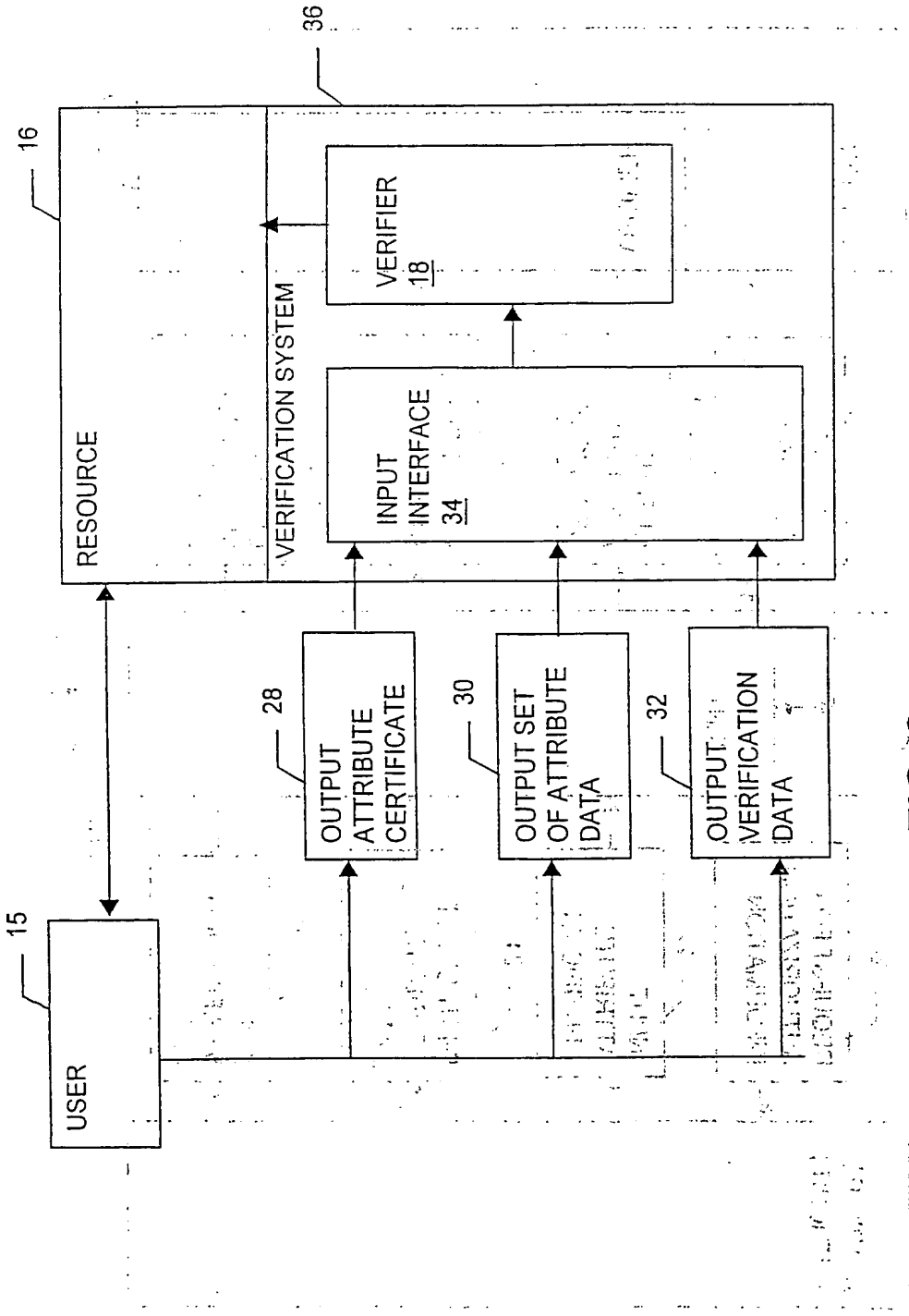

36
16
RESOURCE
VERIFICATION SYSTEM
VERIFIER
18
INPUT
INTERFACE
34
28
OUTPUT
ATTRIBUTE
CERTIFICATE
30
OUTPUT SET
OF ATTRIBUTE
DATA
32
OUTPUT
VERIFICATION
DATA
15
USER

FIG. 2

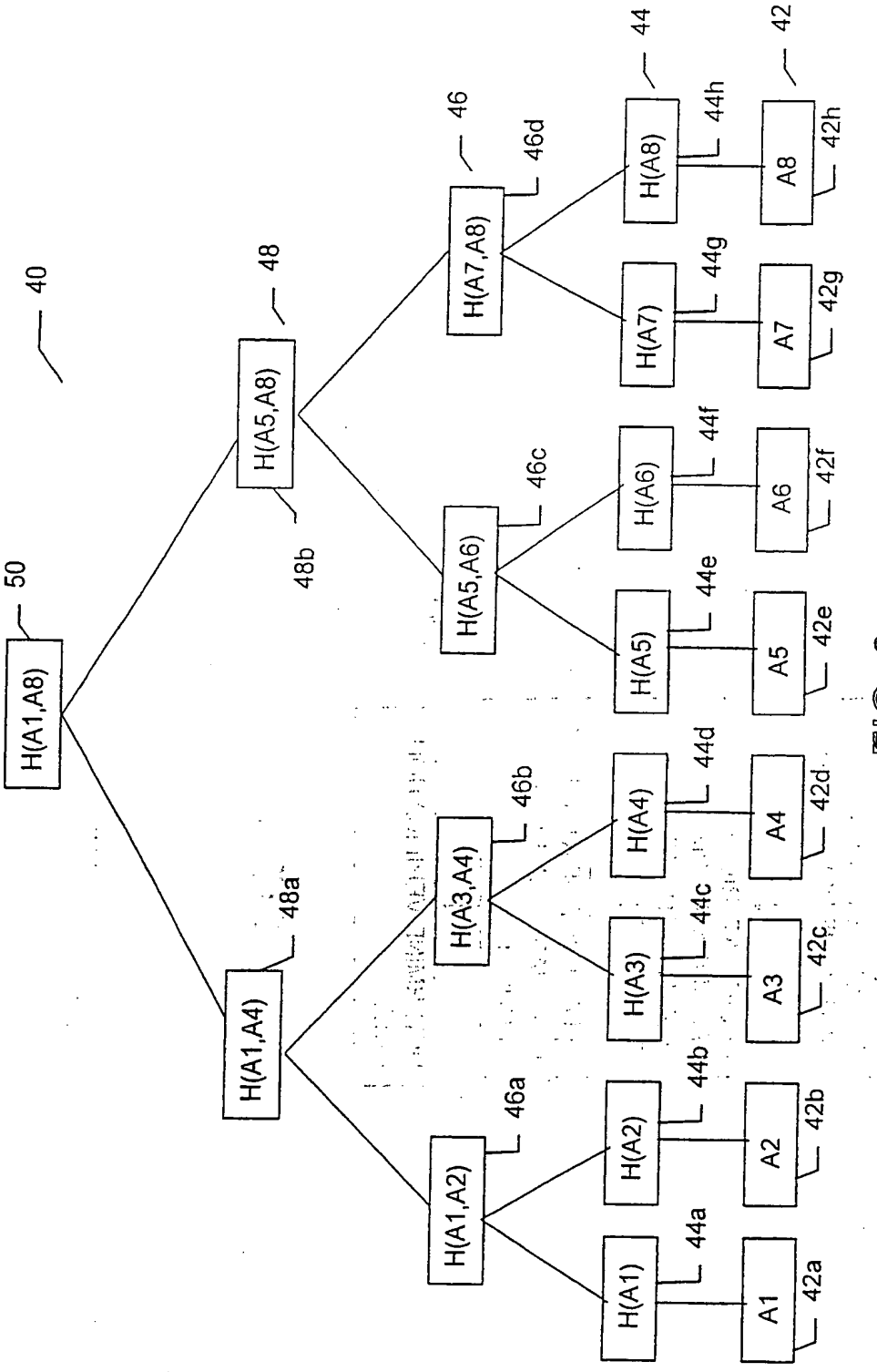


FIG. 3

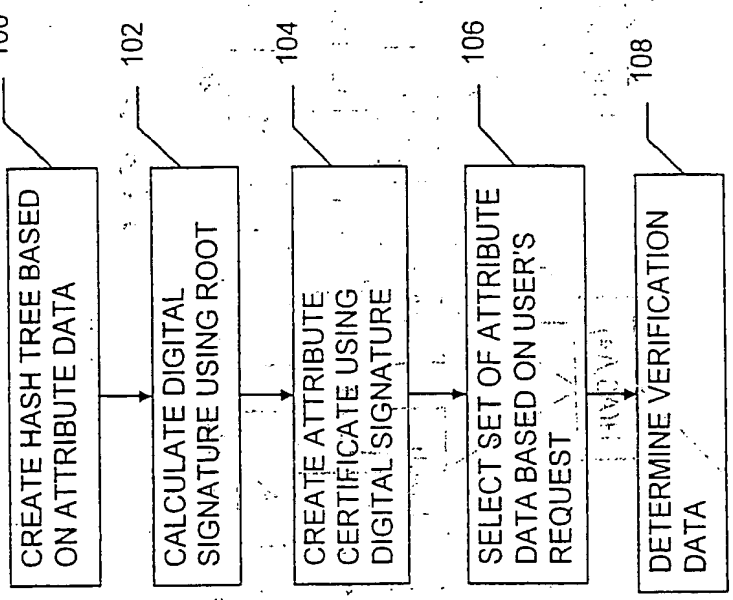

100
CREATE HASH TREE BASED ON ATTRIBUTE DATA
102
CALCULATE DIGITAL SIGNATURE USING ROOT
104
CREATE ATTRIBUTE CERTIFICATE USING DIGITAL SIGNATURE
106
SELECT SET OF ATTRIBUTE DATA BASED ON USER'S REQUEST
108
DETERMINE VERIFICATION DATA

FIG. 4

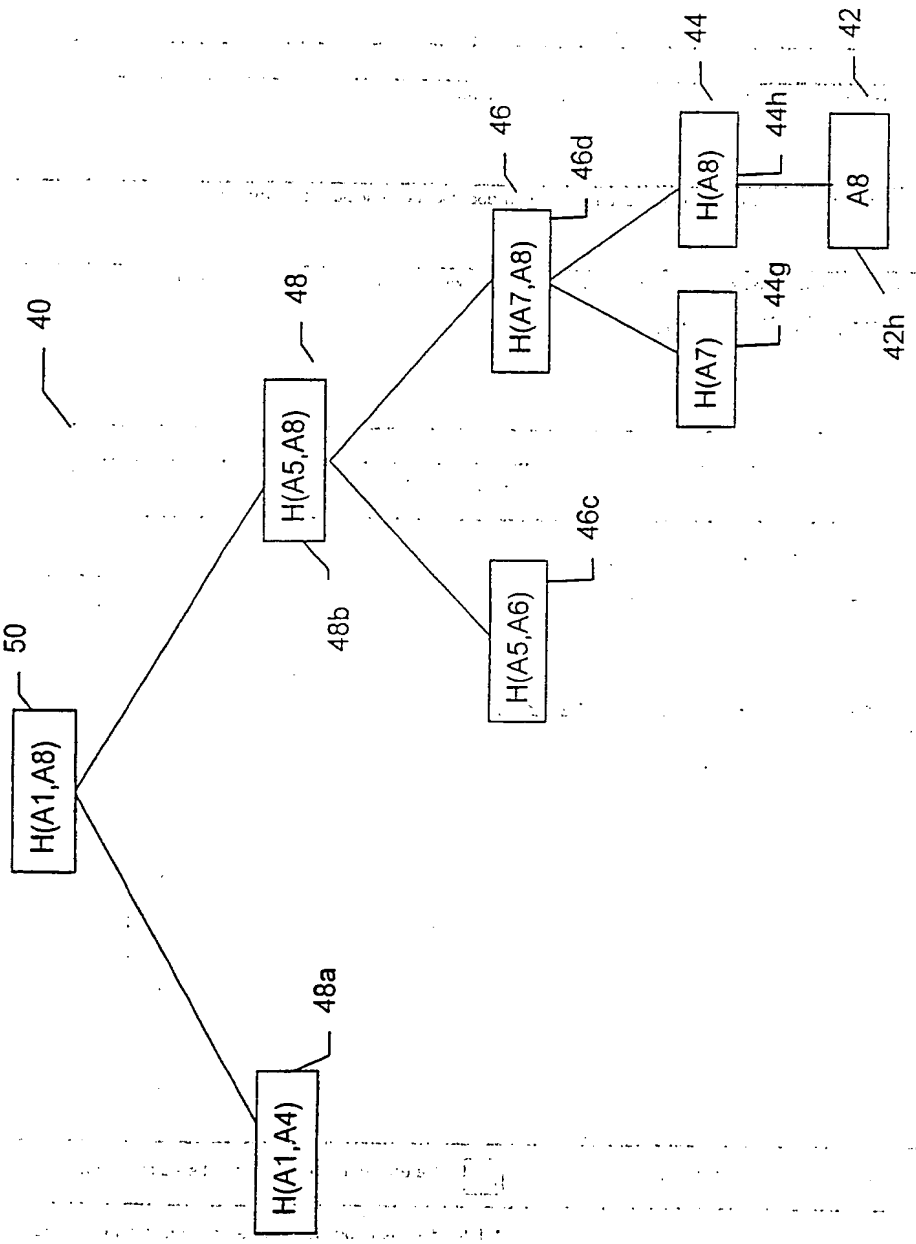

40
50
H(A1,A8)
48
H(A5,A8)
48b
48a
H(A1,A4)
46
H(A7,A8)
46d
46c
H(A5,A6)
44
H(A8)
44h
42
A8
42h
H(A7)
44g

FIG. 5

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/33606

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
E	WO 01 11843 A (SUDIA FRANK W) 15 February 2001 (2001-02-15) abstract figures 1,3 page 24, line 28 -page 32, line 25; figures 4,5 --- -/--	1-8, 10-15, 17-55

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 March 2001	04/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/33606

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	I GASSKO, P GEMMEL, P MACKENZIE: "Efficient and Fresh Certification" PUBLIC KEY CRYPTOGRAPHY '2000, VOL. 1751 OF LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER-VERLAG., 'Online! 18 - 20 January 2000, pages 342-353, XP002164003 Melbourne, Victoria, Australia Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/cs> 'retrieved on 2001-03-27! page 343 -page 348 ---	1-8, 10-15, 17-55
A	LINN J; NYSTRÖM M: "Attribute Certification: an enabling technology for delegation and role-based controls in distributed environments" PROCEEDINGS FOURTH ACM WORKSHOP ON ROLE-BASED ACCESS CONTROL, 29 October 1999 (1999-10-29), pages 121-130, XP002164004 ACM, NY, USA ISBN: 1-58113-180-1 the whole document -----	1-55

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/33606

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0111843 A	15-02-2001	WO 0106701 A	25-01-2001